SECURITY VERSUS SECURITY:
BALANCING ENCRYPTION, PRIVACY, AND NATIONAL SECUIRTY

Jackson Stein

(TC 660H or TC 359T)
Plan II Honors Program
The University of Texas at Austin

05/04/2017

_____

Robert Chesney
Director of Robert Strauss Center
Supervising Professor

_____

Mark Sainsbury
Department of Philosophy
Second Reader

ABSTRACT

Author: Jackson Stein

Title: Security vs. Security: Balancing Encryption, Data Privacy, and Security

Supervising Professors: Robert Chesney, Mark Sainsbury

This paper analyzes the current debate over encryption policy. Through careful evaluation of possible solutions to 'going dark' as well has weighting the costs and benefits of each solution, we found exceptional access to information more harmful than helpful. Today, there seems to be no singular leading answer to the going dark problem. Exceptional access to data and communications is a simple solution for a simple problem, however going dark is very complex, and requires a multifaceted and refined solutions. Widespread encryption forces those listening—whether it is the NSA, FBI, foreign governments, criminals or terrorist—to be much more targeted. As for the going dark metaphor, it seems as though we are not entirely "going dark", and yet we are not completely bright either. There are dark and bright spots coming and going across the technological landscape battling in a perpetual technological arms race. The findings of this paper, ultimately determine there to be no policy that doesn't come without some cost. That said, there are a number of ways in which law enforcement can track criminals and terrorist without weakening encryption, which we determine to be the best direction in any win lose situation. Nevertheless, as technology continues to evolve and encryption capabilities continue to become a part of everyday life for Americans this debate will only grow larger, and we, as a society, must determine how to make the best of it.

Acknowledgements

The completion of this undertaking could not have been possible without the support of friends, family and my immensely knowledgeable supervisors. Firstly, I would like to express my sincere gratitude to Professor Mark Sainsbury for the continuous support of by thesis project, for his patience, wisdom, and encouragement over the last year. Thank you so much for helping me to stay on track and inspiring my research through insightful comments and difficult questions. I would also like to thank Professor Robert Chesney providing indispensable advice, information, and support. Your expertise was essential to the accomplishment of this project. To the Plan II thesis supervisors and directors, thank you for all of your words of encouragement and instruction over these past few semesters. Furthermore, I would like to thank the entire Plan II department for an outstanding educational experience I will appreciate for the rest of my life.

Table of Contents

ABSTRACT ..... **ii**

Acknowledgements ..... **iii**

Introduction **3**

Chapter 1: Background of Today's Debate on Going Dark **6**

The San Bernardino Terrorist Attack 6

Technical and Historical Background: Encryption, Methods, and Backdoors 12

Local Law Enforcement's Solutions to Going Dark 19

Government Mandated Access: Key Escrow Encryption 24

The Dangers of Exceptional Access and Key Escrow Encryption 30

Chapter 2: The Golden Age Of Surveillance **34**

The Effects of the Snowden Revelations 37

Chapter 3: Alternative Solutions to Required Exceptional Access **43**

A Deeper Look into Government Mass Surveillance 46

The Internet of Things 51

Conclusion **60**

Works Cited **62**

Biography **71**

Introduction

What if I told you: anyone could look at your text messages. Anyone could read your emails and listen to your phone calls. They can see where you are, when you are and with whom your calls are made. These are the fears and concerns of many privacy experts today. However, advances in technology have also made it increasingly easy to hide behind digital fortresses. Strong encryption is everywhere, and it seems it is here to stay. United States legislators and law enforcement agencies fear strong encryption technology made readily available to any and all individuals threatens our national security. The tech industry disparages these concerns, arguing that government control violates the privacy of civilians. Although encryption technology has been around for half a century, encryption has gained notoriety in the past decade, as it became a fundamental part of our everyday lives. Every time we log into our email, Facebook, or Internet banking, all of our information is protected using encryption code. It protects our data from malicious hackers, spies, online criminals, and government surveillance. Moreover, the security encryption delivers goes far beyond the individual level. Large databases used by most companies and government agencies can be treasure troves of sensitive information. They can contain customers' personal data such as hospital health records, intellectual property, or even sensitive military information. Many tech companies abide by certain protocols and policies for the prevention of theft or corporate espionage (such as Google, Apple, Amazon, Drop Box, Twitter and many more).

Law enforcement officials raise strong claims concerning strong encryption and its consequences. The FBI, the most vocal government agency, has been concerned there is a widening gap between law enforcement's legal privilege to intercept electronic communications and its practical ability to actually intercept those communications. The Fourth Amendment of the United States Constitution authorizes reasonable searches and seizures, providing law enforcement agencies access to places where criminals hide evidence. Pursuant to judicial warrants these rights are conducted upon a neutral judge's finding of probable cause. However, "Technology has become a tool of choice for some very dangerous people. And, unfortunately, the law has not kept pace with technology and this disconnect has created the significant public safety problem we have long described as "going dark", said FBI director James Comey.[1] This ominous sounding term means that even though law enforcement has the legal authority to intercept and access communications and information pursuant to court orders (according to the 4th amendment) "they often lack the technical ability to carry out those orders because of a fundamental shift in communications services and technologies, allowing the criminals to slip into the dark".[2]

In recent years, Apple and Google have created very strong encryption on their consumer products (iPhones and Androids) by default. This means that millions of people, across the globe, are sending messages with extreme protected communication software that they never chose for themselves. It was gifted to them.

---

[1] Comey, James. The Brookings Institution. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Washington, D.C. October 16, 2014.
[2] FBI.gov, *Going Dark Issue*. April 6, 2016.

Many government officials argue for encryption to be a choice, rather than a requirement to own an iPhone or Android. Moreover, these tech conglomerates didn't strongly advertise these new features. Director Comey also stated "There was always a corner of the room that was dark. Sophisticated actors could always get access, either for devices or for live comms, to encryption. What has happen just in the three years that I have been Director, post-Snowden, is that that dark corner of the room—especially through default encryption on devices—that shadow is spreading through more and more of the room."[3] However, the going dark issue affects a number of law enforcement and national security agencies, and the encryption debate is not viewed the same way across governmental organizations or among the individuals within these organizations. Encryption raising complex question for privacy, security, surveillance, national security, terrorism, and well as economic, political, and social concerns. The needs and resources of government organizations differ, as do their jurisdictional domains. For instance, the resources available to the FBI for defeating encryption may be fewer than those available to the NSA. State and local authorities have access to fewer resources than law enforcement operating at the federal level. However, while the degree of trepidation and operational value may differ among government agencies, there is a general sense by those within both the intelligence and law enforcement communities that they would all benefit if encryption did not present a barrier to investigations. The purpose of this discourse is to analyze the leading arguments from both technology science expert and government officials. The findings of this paper illustrate the

[3] Comey, James. "The FBI's Approach to the Cyber Threat", Symantec Government Symposium: Washington, D.C. August 30, 2016.

inherent problems in government-mandated access to data and communications, as well as provide insight in to alternative outlets for lawful government surveillance that does not weak encryption systems.

Chapter 1: Background of Today's Debate on Going Dark

The San Bernardino Terrorist Attack

San Bernardino—a terrorist attack that killed 14 civilians—subsequently provoked a public battle between the Federal Bureau of Investigation of the United States and the world's largest information technology company[4], Apple Inc.

On December 2, 2015, Syed Rizwan Farook murdered 14 people in a mass shooting and attempted bombing. During the investigation, the FBI recovered Farook's phone, but could not access its contents due to Apple's encryption software. The phone was protected by a four-digit passcode and a self-destruct feature set to erase the phone's Random-Access Memory after 10 failed attempts. The FBI, unable to unlock the phone, asked Apple to create *new* software to bypass the phone's security system. Apple refused.[5] As a result, the FBI filed a suit against Apple for not complying with their search warrant. A public heated debate ensued. However, the case never made it to trial because the FBI was eventually able to open

[4] Largest by revenue
[5] Grossman, Lev. TIME. *Inside Apple CEO Tim Cook's Fight with the FBI. Calif.* March 17, 2016.

the phone using an undisclosed third party technology company. The intensive media coverage accelerated the story to mainstream knowledge, however, less recognized is the impact encryption has on our society. Moreover, San Bernardino is not an isolated incident, but rather, a glimpse into the wider debate between privacy and national security. The propositions posited in this paper weigh theoretical costs and benefits between encryption and national security that may have drastic impacts in our society. Therefore, the aim of this paper is to evaluate, critique and propose leading arguments in the privacy-national security policy debate.

In February 2016, the FBI obtained a court order issued by United States Magistrate Judge, Sherri Pym, in a case called *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203.* This legally obtained warrant mandated Apple to create and provide the requested software. The order was issued under the *All Writ Act of 1789* (which states that U.S. federal courts have authority to issue all writs necessary in aid of their jurisdiction). In doing so, the FBI was not only taking legal action against Apple, it was bringing this dispute out from behind closed doors, and into the public.

However, FBI Director James Comey wanted to make it clear that the FBI isn't against encryption in general. He understands it value and, "I love strong encryption. It protects us in so many ways from bad people. It helps the FBI with our mission, which centers on protecting privacy and fighting hackers."[6] If both

[6] Comey, James. "Expectations of Privacy: Balancing Liberty and Security and Public Safety Center", Study of American Democracy Biennial Conference, Kenyon College: Gambier, Ohio April 6, 2016.

government and the public agree encryption is incredibly useful, why did the FBI appear to be attempting to weaken Apple's software during the San Bernardino investigation, and why is encryption policy still so heavily debated? At the climax of the FBI-Apple debate, FBI Director James Comey stated in a press conference that, "we simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly."[7] Along with the standard four-digit passcode on Apple iPhones, Farook had installed an additional security mechanism with a self-destruct feature set to erase the phone's Random-Access Memory after 10 incorrect entries. After threatening to file a suit against Apple for refusing to grant them access to the phone, the FBI received strong backlash from the tech community, who accused the FBI of trying to force Apple to weaken their encryption software. In response, Director Comey stated in a press conference that, "[the FBI does not] want to break anyone's encryption or set a master key loose on the land…[but] maybe the phone holds the clue to finding more terrorists. Maybe it doesn't. But [the FBI] can't look the survivors in the eye, or [them] selves in the mirror, if [they] don't follow this lead."(Comey, "San Bernardino") Despite this defense, there still remained a number of barriers to forcing Apple to grant them access to the phone.

The first barrier to this forceful request was the fact that Apple's encryption software was end-to-end, which means "the information is (in theory, and as advertised) not capable of being read by anyone who sees it traverse a network

[7] Comey, James. "FBI Director Comments on San Bernardino Matter", LawFare Blog: FBI National Press Office, February 21, 2016.

between the sender and the receiver, including an intermediary service provider, such as Apple. Similarly, device encryption – in which the keys exist only on locked devices – prevents the contents from being read by anyone who does not possess the keys".[8] Only the four-digit passcode known by the phones owner, now deceased, could unlock the information inside. Therefore, the FBI needed Apple to create *new* software to open the phone. As Director Comey had publicly explained, the *new* software would only be used to unlock Farook's phone. While Director Comey is correct that he is not explicitly asking Apple to build a master key system into their software for all devices the new software would give the FBI the ability to break into any device individually. Apple argued that compromising its security, even if only once is akin to providing a backdoor to authorities to gain access to any other Apple device thereafter. In an attempt to explain to Apple costumers the potential dangers of the FBI's request, Cook wrote that "[the FBI] would have the power to reach into anyone's device to capture their data."[9] However, the motivations for Apple's backlash are still up for debate, and there is some subjectivity in evaluating how much of the company's actions were to protect costumers as opposed to the brand. Nonetheless, Apple was strongly supported by other technology conglomerates including Google, Facebook, Twitter, and many more, despite them not having much stake in the San Bernardino case specifically.

A counterpoint to both Apple and the FBI's arguments in the dispute is that rather than giving some kind of key to the FBI, it would seem the FBI could hand the

[8] Blaze, Matt. "U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigation Hearing on "Deciphering the Debate Over Encryption," Washington D.C. April 19, 2016.
[9] Cook, Tim. "Message to Our Customers", Apple.com: Accessed December 2, 2016.

phone to Apple, and have them try and unlock it behind closed doors. The FBI would have the phone unlocked, and Apple would have control of the software and could therefore destroy it after. However, there are also some foreseeable objections to this resolution. (1) What would keep the FBI from returning to Apple with another device, and what are the parameters? (2) And if Apple destroyed the software there created to open each phone afterwards, how much time and resources would the company waste in developing and destroying software, for the FBI? (3) How would this affect Apple's brand financial interests? (4) There is always a possibility of information being leaked.

Similar to this line of reasoning are arguments found in a document from the U.S. Attorneys for the Central District of California Eileen M. Decker, Chief of the Cyber and Intellectual Property Crimes Section Tracy L. Wilkison and Chief of the National Security Division Patricia A. Donahue.[10] In this letter supporting the order to compel Apple's help in unlocking Farook's iPhone, federal prosecutors claim the technology company was playing to the media in an attempt to protect its brand. It reads:

> "Apple and its amici try to alarm this Court with issues of network security, encryption, back doors, and privacy, invoking larger debates before Congress and in the news media. That is a diversion. Apple desperately wants--desperately *needs*--this case not to be 'about one isolated iPhone"(2).

[10] Decker, Eileen, Patricia Donahue, Tracy Wilkison. "Government's Reply In Support of Motion to Compel And Opposition to Apple Inc.'s Motion To Vacate Order", United States District Court For the Central District of California, March 22, 2016.

They claim that work required to comply with the government's request would only take six (out of 100,000) employees two weeks time to complete. Furthermore, the prosecutors claim the argument that weakening the security of one iPhone is a slippery slope to a surveillance state, is "not only false, but also corrosive of the very institutions that are best able to safeguard our liberty and our rights"(2). They claim there is no reason to think that the code Apple writes in compliance with the Order will ever leave Apple's possession. "Nothing in the Order requires Apple to provide that code to the government or to explain to the government how it works." They also claim that Apple is more than capable of protecting its code as it "currently protects (1) the source code to iOS and other core Apple software and (2) Apple's electronic signature (Hanna Decl. Ex. DD at 62-64 (code and signature are "the most confidential trade secrets [Apple] has") (24). Therefore, their argument is, if they can protect some code (of the upmost importance to their company) they can protect any code. From Apple's perspective, why would a company want to risk having more sensitive information to protect if they don't have to?

Regardless of whether Apple's actions were/are entirely constitutional, and regardless of whether their actions are more in line with their own interests than in protecting there customers, in the end, the FBI was able to solve their problem without weakening an encryption systems. The San Bernardino terrorist attack brought national attention to the privacy versus security debate. However, going dark effects all levels of law enforcement.

In continuing this discourse, it is important to address those who may believe this issue is too complex, or too heavily based on technology to be effectively debated in congress, or by the public. In response, let us take a deeper look into both technical and historical background of encryption technology.

Technical and Historical Background: Encryption, Methods, and Backdoors

One rationalization for the FBI/Apple dispute's rapid escalation between is connected to the negative connotation associated with the terms "gaining access"; and its derivative: "backdoor". An exploration of backdoors history shows why many tech experts may be predisposed to reject the FBI's demands. Moreover, too many people have circulated the idea that this issue is to technologically complex to be debated in congress. This is an issue of weighing costs and benefits. In order to do so, we must do our best to fully understand the extent and magnitude of each. However, to claim this policy question should be left to the tech companies and experts alone is illegitimate. To help put that objection to rest, here is a brief on everything one needs to know about encryption from a technical perspective.

It is important to make the distinction, here, between access to Internet networks and communication devices (e.g. iPhones). Encryption is used in both and thus both contribute to going dark. Thus, the government has wanted access to both fore decades, in what has become known as the "crypto wars". This chapter will focus on encryption and mandated access in regards to information on devices

(iPhones/Android), even though themselves are connected through encrypted Internet networks. We will explore the access of the latter in chapter 3. For now, lets explore the history and technology of tradition encryption methods in order to better understand how they can be decrypted, and what the dangers of doing so might be.

The story of backdoor keys begins in the 1970s, when electronic cryptic algorithms boomed with the spread of commercial and government computer systems (it is important to note the NSA's continuous involvement and interest in this technology). As Steve Levy explains in "Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age", the National Bureau of Standards (NBS) released an invitation to propose a candidate for the protection of sensitive, unclassified electronic government data in 1973. [11] NBS received many unsatisfactory proposals, but in 1976 it selected IBM's Data Encryption Standard (DES). The DES is a symmetric-key algorithm for encryption of electronic data built with a 128-bit key.[12] After consulting with the National Security Agency (NSA), the NBS accepted a modified version of the DES in collaboration with IMB. The NSA, however, demanded that the NBS's modifications to the DES design be kept secret. Most notably changing the 128-bit key to a much smaller 64-bit key. Back in those days, this algorithm was almost entirely used solely by the government, financial institutions and corporations (unlike today, where most everyone has an encrypted

[11] Levy, Steve. "How the Code Rebels Beat the Government Saving Privacy in the Digital Age", Penguin Group: New York, 2001.
[12] Tuchman, Walker. "A brief history of the data encryption standard", Internet besieged: countering cyberspace scofflaws. ACM Press/Addison-Wesley Publishing Co. New York. 1997. p. 275–280.

iPhone). As Levy describes, although most cryptographers at the time worked for tech companies or the government, curious academic individuals scrutinized the new encryption standard and its secret modifications. Controversies arose out of these design elements, and the NSA's involvement nourished suspicions about a backdoor.

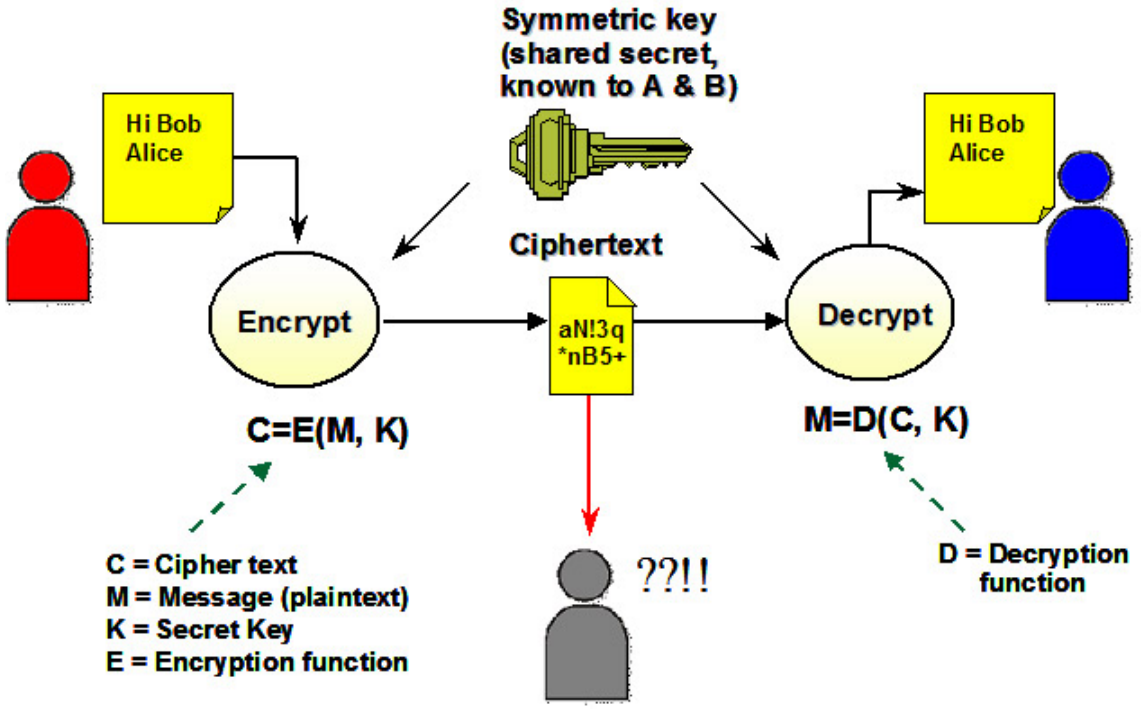
After the DES was published in the *Federal Register*, Martin Hellman and Whit Diffie, two American cryptologists, rightly suspected that the shortened key length and other modified elements were evidence of improper interference by the NSA. They were suspicious the DES was covertly weakened so that the NSA—but no one else—could easily read encrypted messages.[13] This led Diffie and Hellman to question the nature of cryptic schemes. They wondered if a hidden "trapdoor" (later referred to as backdoor) could be built into an encryption system.

Levy explains that Diffie and Hellman realized, "Designing such a system would present considerable challenges, because it would have to resolve a fundamental contradiction. A trapdoor provides a means for those with proper knowledge to bypass security measures and get quick access to encrypted messages; however, the very thought of using a trapdoor in a security system seemed like a nutty risk, precisely because crafty intruders might find a way to exploit it." Just like a physical trapdoor, if your enemies find it, it is rendered useless. However, Diffie and Hellman's ambition and curiosity to build a complex enough scheme to encrypt and decrypt data with a private key developed over the years.

[13] Diffie, Whitfield, Hellman, Martin E. "Exhaustive Cryptanalysis of the NBS Data Encryption Standard*", The Institute of Electrical and Electronics Engineers, Inc.* California: June 1977. 74–84

And by 1978 they published “New Directions in Cryptography” creating the public key encryption scheme widely used today (Levy 88). This paper “was a revelation, a true blow against the empire” Levy enthusiastically explains.

To understand their innovation, let’s examine conventional encryption schemes. Fundamentally, encryption schemes allow for the process of encoding messages or information in such a way that only authorized parties can understand them. Encryption does not prevent interception. It simply prevents the message from being interpreted by the interceptor. One problem Diffie and Hellman found with conventional cryptography was the issue of key distribution. To unscramble an encrypted message between two parties, both parties must exchange a secret decryption key prior to sending the message. In an encryption scheme, information (referred to as plaintext) is scrambled using a mathematical algorithm, generating cipher text (gibberish) that can only be decoded by its recipient. This is not a novel idea. Julius Caesar, for example, used cipher text by moving the last three letters of the alphabet (XYZ) to the front, and sliding the rest of the letters three spaces down. Thus, A would correspond to X, B to Y, C to Z, D to A, and so on, allowing him to write strange groupings of letters that could only be decrypted by those who know the technique, often to protect military secrets. The same idea is used with sending information today, except the encryption keys are digital. The diagram below represents the public key encryption scheme used today, where private conversations can be conducted without prior acquaintance and exchange of private keys.



[14]

In this encryption scheme, Alice and Bob will each have two keys, a public one, which everyone can see and use, and a private one, which they keep secret. Data encrypted with a public key can only be accessed using a private key, and data encrypted with a private key can only be accessed using a public key. To be sure Alice sent the message, Bob can use his public key and Alice's private key to encrypt the message, and upon delivery Bob must use his private key and then Alice's public key to access the message and verify it is from Alice, solving the key distribution problem. Public key cryptography became widely used by government and corporations alike, while continuing to develop in complexity. What distinguishes this method is that the key used to encrypt the message is not the same key used to decrypt the message.

[14] Demopoulos, Ted. *Symmetric Key in Use*, 2008. http://securitycerts.org/review/symmetric-key-in-use.htm

Public key cryptography is often used to secure electronic communication over an open networked environment such as the Internet, without relying on a hidden or covert channel, even for key exchange. Open networked environments are susceptible to a variety of communication security problems, such as “man-in-the-middle attacks”: where an eavesdropper can intercept encrypted messages.

However, since the advent of public key cryptography, the term *trapdoor* has acquired a different meaning, and thus the term "backdoor" is now preferred. As noted earlier, a backdoor is a deliberate mechanism that is added to a cryptographic algorithm (e.g., a key pair generation algorithm, digital signing algorithm, etc.) or operating system, for example, that permits one or more unauthorized parties to bypass or subvert the security of the system in some fashion.

According to Chris Wysopal in his paper, “Static Detection of Application Backdoors”, there are many types of backdoors that can be used today (system backdoors, application backdoors, crypto backdoors). The details of how each work are extensive and insignificant for the purpose of this paper. Wysopal explains, however, “Application backdoors do not require much sophistication to create and there is ample motivation for bad actors to create them. Backdoors are trivial to exploit once the word gets out so response must be very quick. The negative reputation impact to the vendor of the effected software is often much higher than the negative impact from a typical vulnerability.” Thus, backdoors have acquired a negative reputation among tech experts, as backdoor software has been implemented for many nefarious purposes throughout the past decade.

Moreover, in recent years, there are numerous accounts of software created with backdoors that are now considered malware. Two significant examples with discovered backdoor problems include "Back Orifice" and WordPress plug-in. The Back Orifice was a program created in 1998 by the hacker group called "The Cult of the Dead Cow". Back Orifice was a play-on-words for the Microsoft program BackOffice. Back Orifice was created as a backdoor that allowed computers running Microsoft Windows to be controlled remotely over a network. [15]

Another example is WordPress. WordPress is a free and open-source content management system (CMS). It is commonly run as a software package: WordPress.org. However, it has a poor track record of security. WordPress has many plugins available that users download for free. However, sneaky bad actors have easily pirated copies of plug-ins and provide them "free" over the Internet for download. Free plug-ins are surreptitiously patched to include backdoors, which allow for spam and malice attacks. [16] These plug-ins are so widespread that WordPress' own website provides detailed instructions "for beginners" on detecting and deleting hidden malware.[17] Although these cases provide some insight into the many ways the concept of backdoors can be used maliciously, could the right people use a backdoor for a legitimate reason? Or rather, could an encryption system be designed to be both impenetrable to intruders, yet accessible through lawful government requests?

---

[15] Richtel, Matt. "Hacker Group Says Program Can Exploit Microsoft Security Holes" *New York Times* August 4, 1998.
[16] Sineubko, Denis. "Unmasking "Free" Premium WordPress Plugins. *Sucuri Blog*. March 26, 2014.
[17] Editorial Staff, "How to Find a Backdoor in a Hacked WordPress Site and Fix It", *Wpbeginner Blo*g: November 28, 2012.

Local Law Enforcement's Solutions to Going Dark

On the local law enforcement level, there is a growing concern about strong encryption on cell phones connected to a significant number of criminal investigations. Similar to the San Bernardino case, there are countless local criminal investigations effected by strong encryption. Many government officials are calling for a policy that mandates government access to telecommunications. Thus, both local law enforcement and the FBI want to be able to open any phone with a lawful warrant. One proposed solution would be to mandate phone companies to design devices with the capability of being accessed by targeted lawfully government requests.

Cyrus Vance Jr., the New York District Attorney (Manhattan), and prominent mandated access advocate, testified before the U.S. Senate Committee on the Judiciary in July of 2015. In response to Apple and Google installment of robust encryption software on its products by default, Vance argued, "requiring phones to be manufactured so that they would be accessible to law enforcement through lawfully obtained search warrants"(Vance 17). Although this testimony never uses the term "backdoor", on a technical level there is no other way to gain "access" to encrypted data other than creating a backdoor. Vance also states, "I am proposing here…a return to the balanced approach in place prior to the introduction of iOS 8" (Vance 17). Regardless of the merits and concerns for both privacy and security, technology is a tempestuous train of progress driving forward, unlikely persuaded

to “return” or backtrack. Nevertheless, how does backdoor technology work, and what are some of its advantages (advocated for by the law enforcement) and what are its disadvantages?

Moreover, Vance claims “It is not hyperbole to say that beginning in September 2014, Americans conceded a measure of their protection against everyday crimes to Apple and Google’s new encryption policies” (Vance 4). He is referring to the fact that, Apple and Google significantly increased the encryption capabilities of their products shortly after Edward Snowden’s leak of NSA classified global surveillance programs. One of the reasons law enforcement is frustrated with Apple and Goggle’s implementation of robust encryption systems, is that it was done so by default. Many government officials argue this is unconstitutional, and that giving consumers a chance to choose between using strong encryption or not, would be more appropriate. Perhaps if consumers had a choice, many would choose not to use it, as people are inherently lazy and if it took extra steps to use, perhaps the average American would find the task superfluous. This logic is impractical, as Apple and Google appear to have no intention of considering this modification to their business model. They implemented this security strategy for both proprietary and economic purposes, as well as for the security of their customers. Hypothetically, if they did offer encryption not by default, any criminal or terrorist not utilizing this security feature, would most likely be caught or thwarted long before the going dark issue would apply for a number of reasons relating to their significant lack of intelligence.

Moreover, there are a number of concerns with having a significant portion of people not using secure methods of communication, as we will see. Nevertheless, not offering encryption by default seems impractical to be successfully implement, as well as not being a meaningful solution to going dark concerns. As we have seen on the local law enforcement level, arguments surrounding the going dark issue are persuasive because they are tangible. Law enforcement can cite real cases where technology has separated evidence from crimes and criminals from persecution. However, it is important to keep in mind that encryption and going dark affects all levels of security, from local law enforcement to the NSA, and as we rise, so does the complexity of the issue. It becomes less concrete and more abstract and hypothetical.

Yet, Government officials, such as Vance, argue that highly secure encrypted communication poses national security risks. According to FBI Director Comey, law enforcement is seeing more and more cases where it believes significant evidence can be found on a phone, tablet, or laptop, and that this evidence that may make the difference on whether the offender is convicted or acquitted.[18]

Tim Cook publicly acknowledged its security modification and its impact on law enforcement. According to Cook in a message posted on Apple Inc.'s website:

> "On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your

[18] Comey, James "Directory Comey Discusses Investigative Challenges in Light of New Methods of Electronic Communications" Fbi.org. March 1, 2016.

> passcode… Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."[19]

Law enforcement is extremely concerned about the serious threat posed by the use of robust encryption products that do not allow for authorized access or the timely decryption of critical evidence, obtained through lawful electronic surveillance and search and seizure.

Comey states, "If at the end of the day the American people say, 'you know what, we're okay with that portion of the room being dark. We're okay with'—to use one example—"the FBI, in the first 10 months of this year, getting 5,000 devices from state and local law enforcement and asked for assistance in opening them, and in 650 of those devices being unable to open those devices." That's criminals not caught, that's evidence not found, that's sentences that are far, far shorter for pedophiles and others because judges can't see the true scope of their activity" (Comey, "The FBI's Approach to the Cyber Threat"). To put matters in contexts, "the New York County District Attorney's Office handles more than 100,000 criminal cases each year, which is more than all of the cases handled by the Department of Justice nationwide. And the range of those cases is broad – from murder, rape, and robbery, to identity theft, financial fraud, and terrorism" (Vance 1), states Vance in a testimony before the United States Senate Committee on the Judiciary. He explains how people "live their lives today on their smartphone" and use them for "emailing,

[19] Cook, Tim. "We Believe Security Shouldn't Come at the Expense of Individual Privacy" Apple.com/Privacy. Accessed on October 23, 2016.

texting, taking pictures, posting pictures, shopping, conducting business, and searching the web" (Vance 2) and to investigate those 100,000 cases without access to their phones makes it nearly impossible.

To illustrate this point, Vance describes how a father of six was murdered in Evanston, Illinois. The city police believe he was robbed of a large sum of money just prior to his murder, however no were no witnesses or surveillance footage of the killing. However, an iPhone 6 and a Samsung Galaxy S6 Edge running Google Android were found at the scene. Believing that relevant evidence might be stored on them, the Cook County prosecutors served Apple and Google warrants to unlock the phones. However, due to the phones' end-to-end encryption, never company was capable of unlocking them, and the homicide remains unsolved (Vance 4). Vance continues to explain how his Office "obtains smartphone evidence to support all types of cases – homicides, sex crimes, child abuse, fraud, assaults, robberies, cybercrime, and identity theft" (Vance 2). Disturbingly, it's no stretch of the imagination that sexual offenders especially, might take photos and videos of their acts, and store them on computers and smartphones. Vance states that "Between October 2014 and June 2015, 35 percent of the data extracted from all phones by [his] Office was collected from Apple devices; 36 percent was collected from Android devices. That means that when smartphone encryption is fully deployed by Apple and Google, 71 percent of all mobile devices examined—at least by [his] Office's lab—may be outside the reach of a search warrant."

As serious as these problems may be for the District Attorneys office, it is important to note that this testimony was written in July of 2015. Thus, it was

before the FBI was able to crack the phone from the San Bernardino case with the aid of a third party. Law enforcement has claimed it has the ability to open any device running the same operating system (iOS 9). That being said, a significant portion of the collected phones Vance has mentioned in the testimony should be, therefore, accessible. Law enforcement shouldn't blame Apple or Google for difficulty collecting criminal evidence committed until around 2016 (when the new iOS 10 was released). Nevertheless, more and more criminals, now using the updated software, are digitally safe from conviction. In 2016 Vance stated, "In my office alone, we now have 270 lawfully-seized iPhones… that are completely inaccessible."

In the San Bernardino case, the FBI claimed they only wanted to access one particular phone contributing to a terrorist investigation. Forced to hack into the phone, and presumably gaining the ability hack into any phone of made with the same operating system, the going dark problem remains. Many of those in government agencies are calling for mandating access to encrypted devices. So the question becomes: can we design a system that would allow government access to these devices? How might it look, and what consequences will it bring?

Government Mandated Access: Key Escrow Encryption

This is the question many leading law enforcement officials are asking today, although it is not a new idea. In 1993 the U.S. created the Clipper Chip, a chip developed and promoted by the NSA. It was intended to be built into commercial

phones sold by telecommunication companies, such as AT&T. Matt Blaze, a cryptography researcher at the University of Pennsylvania mentions, "The government has stated that the goal of the [Clipper chip software] is to make a strong cipher available for legitimate use without supplying criminals and other adversaries with a tool that can be used against American interests or to hide illegal activities from law enforcement."[20]

This example is interesting for multiple reasons. The Clipper Chip was a piece of hardware that uses encryption algorithms similar to the Diffie-Hellman key exchange algorithm. This is somewhat ironic in that the government agency itself developed a tamperproof product that a decade earlier it was fighting to limit. In addition, there is irony in the fact the NSA built technology that is analogous to what FBI director James Comey is currently criticizing the tech industry for creating. When talking about Apple products, Comey states, "it takes us to a place of absolute privacy that we have not been to before where the balance we have long struck is fundamentally challenged." (James Comey, "Expectations of Privacy: Balancing Liberty, Security, and Public Safety"). However, the Clipper Chip *did* have a built in backdoor allowing government access to the phones data. This is an example of what is called a *key escrow encryption* system. In theory, once the key is compromised, all of the data the key protected is vulnerable. This method differs from *end-to-end* encryption, which is how Apple protects its products information stored on devices and in transit, meaning only the user can read the message. An analogy would be the way modern ships use compartmentalized hulls to avoid

[20] Blaze, Matt. "Protocol Failure in the Escrowed Encryption Standard", AT&T Bell Laboratories, August 20, 1994. p. 59–67.

capsizing. If the ship's hull is completely hollow, one break in the wall and the entire ship will be flooded with water. However if the hull is compartmentalized so there are many "room" inside the hull of the ship, if one wall is pierced, only one room will be filled with water. The same goes for end-to-end encryption. If a key is compromised, then only the data from that access point can be stolen, and the system as a whole is protected. Apple uses and encryption key, your passcode, to encrypt the device and all information stored on the device.

The reason it is difficult to break open an iPhone is because once the key is used to open the device, it is not stored on the device, but immediately destroyed. Moreover, iPhones only allow a few attempts to guess the passcode before locking up. Therefore, a hacker cannot use "brute force" to open the phone: using a machine to guess millions of passcodes in seconds, because after a few wrong guess the hacker is locked out. Furthermore, Apple has end-to-end encryption of iMessage and FaceTime, meaning communications through these channels cannot be intercepted and decrypted, as an eavesdropper would not have access to any decryption keys. By contrast, *key escrow encryption* is an arrangement in which an authorized third party holds the keys needed to decrypt encrypted data.

In this case, the built-in Clipper chips would hold the keys available to government agencies when needed. It seemed unlikely consumers would have had any idea what they were purchasing. Nevertheless, Matt Blaze, a Cryptography researcher at Princeton University, in 1994 published the paper *Protocol Failure in the Escrowed Encryption Standard*. This paper pointed out how vulnerabilities pervaded the Clipper chip. In his research paper, Matt Blaze states that, "several

approaches can easily circumvent the law enforcement access mechanism, with a range of practicality and tradeoffs." In other words, the system was easily exploitable by hackers. When considering if the software's architecture could be improved or modified, Blaze concludes that, "It is not clear that it is possible to construct an EES (escrow encryption standard) system that is both completely invulnerable to all kinds of exploitation as well as generally useful."

Matt Blaze's study was able to find significant vulnerabilities in this specific example of a key escrow encryption system, however could the government work with tech companies today to develop a modern, more secure version? This is the solution that many Law enforcement officials have asking for. They believe it to be the best constitutionally acceptable answer to the going dark dilemma. However tech experts claim any key escrow system is inherent flaw, as the Clipper Chip is just on of many examples.

There are two principle obstacles for a third-party escrow encryption system according to a group of computer scientist at MIT in their paper called "Keys Under Doormats: Mandating Insecurity by requiring Government Access to All Data And Communications.[21] The first is that "although the mode of encrypting a symmetric key with a public key is in common use, companies are aggressively moving away from it because of a significant practical vulnerability: if an entity's private key is ever breached, all data ever secured with this public key is immediately

[21] Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Glimore, Mathew Green, Susan Landau, Peter G. Neumann, Ronald Rivest, Jeffrey Schiller, Bruce Schneier, Michael Specter, and Daniel Weitzner. "Keys Under Doormats: Mandating insecurity by requiring government access to all Data Communications," Massachusetts Institute of Technology, Cambridge. July 6, 2015. p. 12

compromised. Because it is unwise to assume a network will never be breached, a single failure should never compromise all data that was ever encrypted." Companies are, therefore, using "forward secrecy": a system in which a new key is generated with each transaction and discarded afterwards. Thus, there is much less information vulnerable to attackers. "When a system with forward secrecy is used, an attacker who breaches a network and gains access to keys can only decrypt data from the time of the breach until the breach is discovered and rectified; historical data remains safe" (Abelson 12).

The other obstacle is the procedural difficultly in designing a third-party key escrow system. Who would control the keys? Within the United States, the FBI would most likely hold the private key with access to data warranted by judicial mechanisms, allowing it to be employed for a number of federal, state, and local law enforcement cases. However, as Google and Apple are massive global companies, with Androids and iPhones all across the world, this leaves unanswered questions about what would happen outside a our nation's borders. This MIT study further poses the question:

> "Would German and French public- and private-sector organizations be willing to use systems that gave the US government access to their data — especially when they could instead use locally built systems that do not? What about Russia? Would encrypted data transmitted between the US and China need to have keys escrowed by both governments? Could a single escrow agent be found that would be acceptable to both governments? If so,

would access be granted to just one of the two governments or would both need to agree to a request?"(12)

Furthermore, there are broader economic issues to consider. Democratic economic growth is capable due to innovations in science, technology and business processes. Today, digital products and services are imbedded with new apps and web services. "Increasingly these are also "social Countries that require these new apps and web services to have their user-to-user communications functions authorized by the government will be at a significant disadvantage. At present, the world largely uses US apps and services, rather than the government-approved ones from Russia and China. This provides enormous leverage to US businesses."

Although much of the debate in the media and among privacy advocates has focused on whether Director Comey is asking for companies like Google and Apple to create backdoors, no formal proposals have emerged from the FBI or other members of the law enforcement and intelligence communities. In July 2015, Director Comey stated in Senate Judiciary and House Intelligence Committees that "while there has not yet been a decision whether to seek legislation, we must work with Congress, industry academics, privacy groups, and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months" (Comey, "Going Dark"). Director Comey has also asked that rather than pursue a legislative mandate, instead he advocates to "continue conversations with industry" to find voluntary solutions. Furthermore, he has called on the private sector for help in identifying solutions that provide that

maintain public cyber security without impeding lawful government surveillance efforts.

The Dangers of Exceptional Access and Key Escrow Encryption

In light of many technological security failures of today, many computer scientists and security experts argue the need for more security technology and stronger encryption across the board. In 2014 and 2015, for instance, "unnamed hackers – probably the Chinese government – stole 21.5 million personal files of U.S. government employees and others", explains Bruce Schenier, a computer security professor at Harvard University. He claims these hackers wouldn't have obtained this data if it had been better protected by encryption.[22] Many similar large-scale criminal data hacks have been made both either easier and more damaging because data wasn't encrypted for companies such as Target, TJ Maxx, Heartland Payment Systems, and so on.

One of the most remarkable backdoor hacking pulled off in 2004 has become known as "The Athens Affair". Vodafone, a British multinational telecommunications company and Greece's largest cellular service provider, built backdoor access into Greece's cell phone network for the Greek government. In March of 2005, it was discovered that the Prime Minister of Greece's cellphone was being bugged, as well

[22] Schneier, Bruce. "Security or Surveillance?" Lawfare Blog, February 1, 2016. Accessed on September 12, 2016.

as the mayor of Athens and at least 100 other high-ranking dignitaries.[23] Although the identity of perpetrators debated (many believe it to be United States' handy work), these clever perpetrators either penetrated the network from outside or from the inside with the help of a mole. We can only image the store of incredibly sensitive political and diplomatic discussions, not to mention personal information that was routinely overheard and probably recorded.[24] Because these phones were manufactured with backdoors intended for government use and control, the hackers were able to break into the telephone network and subvert its built-in wiretapping features for their own purpose.

Another significant breach of security occurred in 2010, when the NSA and its British counterpart GCHQ, or Government Communications Headquarters, hacked into the computer network of the largest manufacturer of SIM cards in the world, Gemalto, and stealing encryption keys used to protect cellphone communications. Documents leaked by Edward Snowden claimed these spy agencies were able to manipulate billing records to conceal their own activity and had access to authentication servers to decrypt both voice calls and text messages. [25] As a result, the NSA and GCHQ compromised the security of potentially billions of phones worldwide. Moreover, the only way to address the security compromise is to recall every SIM sold by Gemalto, which would be exceedingly expensive and difficult.

---

[23] Prevelakis, Vassilis, Diomidis Spinellis, "The Athens Affair," IEEE Spectrum, June 27, 2007.
[24] Vassilis Prevelakis, Diomidis Spinellis, "The Athens Affair," IEEE Spectrum, June 27, 2007.
[25] https://theintercept.com/2015/02/19/great-sim-heist/

Furthermore, in 2013 we learned the Chinese Government hacked Google's team that interacts with government surveillance requests. The Chinese Government breached Google's database in order to gain access to classified information about suspected spies, agents, and terrorist under US government surveillance. David W. Aucsmith, senior director of Microsoft's Institute for Advanced Technology in Governments, claims this is brilliant counterintelligence. He sais "you have two choices: If you want to find out if you agents, if you will, have been discovered, you can try to break into the FBI to find out that way. Presumably that's difficult. Or you can break into the people that the courts have served paper on and see if you can find it that way. That's essentially what we think they were trolling for."[26] This type of breach of information would not have been possible with more robust forms of security systems. Google has a team of 300 engineers just for cyber security. If Google and Microsoft, both leaders in the technology industry, cannot protect their data, what hope is there for the rest of us, if we start weakening our encryption systems?

The list goes on. Syria's computer hacking group SEA (Syrian Electronic Army) hacked Skype's Facebook, Twitter and blog, posting an SEA related picture and telling users not to use Microsoft's e-mail service Outlook.com, claiming that Microsoft sells user information to the government.[27] They also hacked the official Microsoft Office Blog, posting several images and tweeted about the attack.

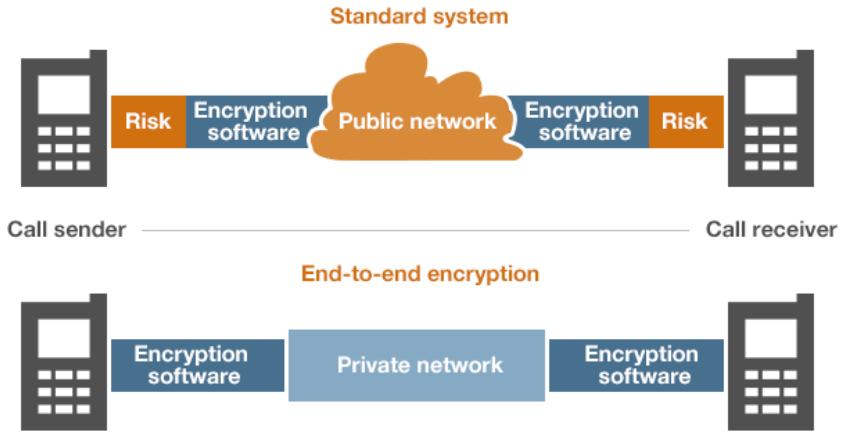
---

[26] https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html?utm_term=.5c67f1969fd6

[27] Shira Ovide (1 January 2014). "Skype Social Media Accounts Hacked by Syrian Electronic Army". *Wall Street Journal*. Dow Jones. Retrieved 22 March 2015.

Strong security and the protection of sensitive information is paramount with regards to fair and ethical business practices today. Not only do businesses in the banking and finance industries have a legal obligation to prevent inside trading, some tech experts argue even lawyers, "have an ethical obligation to protect your communications, and if [they] don't, [they] are engaging arguably in unethical conduct."[28]

In conclusion, when it going dark, it seems impossible for the government to practically solve the going dark solution by weakening encryption; by using any sort of encryption scheme. Hypothetically, even if the Government was successful in gaining access to Apple and Google i.e., there will always be other means by which nefarious actors can secure their communications. There are many encryption apps available for download, and new ones are sprouted every day. Most notable is Whatsapp, a free instant messaging application that enables end-to-end encryption for both messaging and voice calls.



[29]

[28] (22:22).
[29] This diagram illustrates the difference between standard encrypted instant messaging and Whatsapp end-to-end messaging.

Moreover, on the Internet side of the matter, there are dozens of VPN's (virtual private networks) free for download. VPNs cloaks and encrypts web-browsing signals, making online activity completely illegible to any eavesdropper. They also manipulate IP addresses, making it appear as though one is browsing the web from a machine or location different than where they truly are operating.

Ultimately, it seems weakening the system to allow "good" guys access (our government, supposedly) will also allow "bad" guys access. There cannot be one without the other, and there is no to discriminate intent. Trying to decide on how best to solve the going dark problem seems to produce more questions then answers. However, this analysis shows strong widespread encryption protects us from malicious hackers and foreign governments, and we should consider any and all other possible solutions before considering weakening these systems to required mandated access.

Chapter 2: The Golden Age Of Surveillance

As we have discussed, mandating access fails as an optimal solution to going dark. Many tech experts believe this is simply technologically impossible. This leaves government officials, lawmakers, and citizens in a legally and ethically perplexing position. However, there are many that believe the going dark issue is not as threatening as the government agencies claims. There may not be one be all

end all solution, however there are a number of promising avenues available to make the best of our current situation.

As tensions have dissipated in the media since the Apple dispute in 2015, law enforcement is continuing its search for an answer to the "going dark" problem. Although "going dark" is an issue that seems to affect all levels of nation security, the FBI has been the leading voice with James Comey, in particular, in urging tech corporations, Congress and the public to help tackle this issue. To be clear, James Comey asserts his appreciate the importance of strong encryption. He called strong encryption "a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security" and said that the FBI supports and encourages secure networks to prevent cyber threats to the national critical infrastructure, intellectual property, and private data.[30] But he also explained that "the benefits of our increasingly digital lives have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage."[31] Yet, he frequently and repeatedly used rhetoric such as, "we must continue the current public debate." Strong encryption is clearly a significant issue to the FBI director as he continuously devotes his time and energy to "continuing the public debate", but to what end? Rather than continuing a real debate, perhaps it's a matter of maintaining public awareness of the threat. His goal, most likely, is to create more cooperation between the tech companies and the government, by including the

[30] https://www.fbi.gov/news/stories/director-comey-discusses-investigative-challenges-in-light-of-new-methods-of-electronic-communication
[31] Ibid.

public (Apple/Google customers) in the conversation. The FBI director has devoted significant time and energy into this awareness campaign, and it is our job to fully and impartially evaluate the issue, if a policy is to be voted on in the near future. Thus far, we have discussed the technological issue related to going dark. Let us now examine the more political inner workings of the corporate/government affairs, national security and surveillance.

Christopher Soghoian, the principal technologist at the American Civil Liberties Union, provides an interesting insight on the historical context of this debate in a lecture at the International Forum on Cybersecurity. He says, "for more than a hundred years telephone companies have helped governments to spy… the governments of major countries have known that for whoever they wanted to spy on, they could just ask one of their friendly telecommunications companies"[32] because more many of these years, these were state controlled entities. As technology advanced from the telegraph, to the telephone, to text messaging and so on, the governments needs followed. Soghoian explains that because there was a "friendly" relationship between the telephone companies and governments "the telephone companies ensured that their products were designed for surveillance."[33] So each time a telecommunications company offered a new service, they made sure that it could be surveyed and the governments could request access. This was framed in the U.S. by the Communications Assistance to Law Enforcement Act (CALEA), which required telephone companies and others to ensure that their networks could be wiretapped, with appropriate legal process, as network

[32] https://www.youtube.com/watch?v=kqWn-DF-ln8 (1:45)
[33] Ibid (2:10)

technologies moved from analog to digital.[34] However as we have observed, things have changed. Recently, Silicon Valley tech companies, namely Apple, have captured portions of the communication market, by creating and controlling the phones and computers themselves, and consequently have obtained consumers communications.

The problem for governments is the fundamental difference in philosophies between these tech companies and the telephone companies of the past. Soghoian notes, "the phone companies first and foremost see government as a partner in part because they're so heavily regulated and licensed that they need the government for permission to do everything" while companies like Apple do not. This oversimplification presents significant insight into the recent uproar on both sides, and (along with the 9/11 terrorist attack) helps to explain the governments revamped surveillance tools as well as their estrangement from major tech companies.

The Effects of the Snowden Revelations

In recent years we have witnessed an advancement of both security capabilities and surveillance capabilities—making it possible to track and learn about individuals on a mass scale. These efforts and resources have not been without results, however, as NSA director Michael S. Rogers says that over 50

[34] Ben Adida, Collin Anderson, Annie Anton, et al., "CALEA II: Risks of Wiretap Modifications to Endpoints," (May 17, 2013).

terrorist plots have been foiled since 9/11.[35] However, Former NSA contractor Edward Snowden's disclosures brought to light many of the mass surveillance tools and techniques the government has established since the passage of the Patriot Act in the aftermath of the September 11 attacks. The Patriot Act signed into law by President George Bush on October 26, 2001, was established to enhance surveillance procedures in order to track and catch terrorists. Other subsequent national security acts followed such as the PRECISE Act and the FISA Amendment Act's PRISM surveillance program. Moreover, an additional surveillance agency was created in 2002: the United States Department of Homeland Security. In 2016, this agency alone was allocated a net discretionary budget of $41.2 billion.[36] Since the signing of the Patriot Act 15 years ago, Snowden revealed a number of procedures and tools developed by the NSA, in particular, which have resulted in mass surveillance amplifications. Here are some of the most significant revelations from Snowden's leak:

1) **MetaData**: His report revealed that a secret court order requires Verizon to give the NSA the phone numbers, duration time, routing information and other details for any calls made within the United States or between the United States and other countries (however, it does not require Verizon to provide a record of actual conversations).[37] This revelation is still one of the most controversial, and

[35] http://abcnews.go.com/Politics/nsa-director-50-potential-terrorist-attacks-thwarted-controversial/story?id=19428148
[36] https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf
[37] https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

the legality of these request are still being questioned. Moreover, Verizon is not alone; AT&T and Sprint received similar court orders as well as many credit card companies.[38]

2) **PRISM:** Under section 702 of the FISA Amendments Act of 2008, PRISM requests at least nine major Internet companies to turn over any data that match court-approved search terms.[39] The NSA can use these PRISM requests to target communications that were encrypted when they traveled across the Internet, to focus on stored data that telecommunications filtering systems discarded earlier, and to get data that is easier to handle.[40] A Google spokesperson told the *Guardian* that, "Google does not have a back door for the government to access private user data."[41] Snowden's report indicated that PRISM is "the number one source of raw intelligence used for NSA analytic reports."[42]

3) **GCHQ:** The British spy agency taps fiber optic cables all over the world to intercept data flowing through the global Internet. The GCHQ works closely with the NSA sharing data in a classified program codenamed "Tempora".[43]

---

[38] https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[39] Barton Gellman & Ashkan Soltani (30 October 2013). "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". The Washington Post. Retrieved October 31, 2013.
[40] Siobhan Gorman & Jennifer Valentiono-Devries (20 August 2013). "New Details Show Broader NSA Surveillance Reach - Programs Cover 75% of Nation's Traffic, Can Snare Emails". The Wall Street Journal. Retrieved August 21, 2013.
[41] http://mashable.com/2013/06/06/prism-tech-companies-data-mining/#dmoEVODopZqA
[42] Staff (June 6, 2013). "NSA Slides Explain the PRISM Data-Collection Program". The Washington Post. Retrieved June 15, 2013.
[43] https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?CMP=twt_fd

4) **XKeyscore:** is a tool the NSA uses to search "nearly everything a user does on the Internet" through data intercepted across the world. In Snowden's leaked documents the NSA describes it as the "widest-reaching" system to search through Internet data.[44] Xkeyscore operates in over 700 serves worldwide.

5) **Tailored Access Operations (TAO):** When the surveillance tactics listed above fail to provide adequate information, the NSA uses a hacker team codenamed "Tailored Access Operations" to infect targeted computers worldwide with malware. Snowden's leak revealed that over 50,000 computers have been hacked worldwide.[45]

6) **NSA Tapped Yahoo and Google Data Centers:** The NSA broke into the main communications links that connect Yahoo and Google data centers around the world. According to Snowden's report, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans. The NSA uses a tool called MUSCULAR, in a joint operation with the British agency GCHQ to copy entire data flows across fiber-optic cables that carry information among the data centers of Yahoo and Google.[46] Interestingly, the NSA

---

[44]See Snowden, Edward, "XKeyscore", xkeyscore@nsa, February 25, 2008. Accessed on November 8, 2016. https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf

[45] See Derix, Steven. "NSA Infected 50,000 Computer Networks with Malicious Software", nrc.nl: November 2013. Accessed January 14, 2017.https://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487

[46] https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.5055f16c5db6

was already requiring gaining access to Yahoo and Google through the undisclosed PRISM program.

7) **DISHFIRE:** Through this program, the NSA was collecting 200 million text messages per day. The agency described this method as a "goldmine to exploit" for all kinds of personal data.[47] According to the *Guardian* article, the NSA uses these messages to extract the senders' and recipients' personal data such as location information, financial activity and contact details.[48]

About a year and a half after these disclosures, Apple developed iOS 8 with default encryption of the password-protected contents of its devices in the mobile operating systems.[49] This operating system encrypts the data stored locally on the phone, in transit, and stored on Apple's servers.[50] Google quickly followed suit by announcing Lollipop, its next version of Android OS. This new operating system would also enable encryption by default.[51] A few months later, WhatsApp, the popular free instant messaging application for smartphones—now owned by Facebook—announced it would implement TextSecure, an end-to-end encryption

---

[47] See Ball, James. "NSA collects millions of text messages daily in 'untargeted global sweep" The Guardian: January 16, 2014. Accessed on November 23, 2016.
[48] Ibid.
[49] See Sanger, David. "Signaling Post-Snowden Era, New iPhone Locks Out NSA," The New York Times, September 26, 2014,
[50] Apple, Inc., "iOS Security Guide: iOS 8.1 or later," October 2014
[51] Timberg, Craig. "Newest Androids will join iPhones in offering default encryption, blocking police," The Washington Post, September 18, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newestandroids-will-join-iphones-in-offering-default-encryption-blocking-police/.

software.[52] In March of 2015, Yahoo developed source code for Yahoo Mail that encrypts messages.[53] What we are seeing is an unrelenting technological arms race.

Moreover, in June 2015 the United States Senate approved the USA Freedom Act, which reformed several provisions of the Patriot Act from 2002.[54] The Act imposed some limits on the bulk collection of telecommunication metadata on U.S. citizens by the NSA. According to Jameel Jaffer of the American Civil Liberties Union, "This is the most important surveillance reform bill since 1978, and its passage is an indication that Americans are no longer willing to give the intelligence agencies a blank check. It's a testament to the significance of the Snowden disclosures and also to the hard work of many principled legislators on both sides of the aisle."[55]

By amending section 215, the USA Freedom Act required the phone data to remain with the telecommunications companies, rather than directly by the NSA. The NSA would have to go to the FISC (Foreign Intelligence Surveillance Court) court to get access. The government would argue that by not directly holding large sums of data themselves, this does not amount to mass surveillance. Moreover, even when they did hold all of the data themselves, the government claims they would only access it for targeted searches. Even so, that much data appears to be an imbalance of power at their fingertips. Nevertheless, these provisions only apply to

---

[52] See Greenberg, Andy. "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," WIRED, November 18, 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.
[53] See Stamos, Alex. "User-Focused Security: End-to-End Encryption Extension for Yahoo Mail," Yahoo Blog, March 15, 2015,
[54] https://www.congress.gov/bill/107th-congress/house-bill/3162
[55] See Siddiqui, Sabrina. "Congress Passes Surveillance reform in vindication for Snowden" https://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden

phone records. The NSA can continue to collect bulk data from the Internet.[56] The Act preserves "the intelligence community's ability to gather information in a more focused way"[57] as we have examined above.

In conclusion, Snowden's disclosures revealed disturbing truths about U.S. and foreign government mass surveillance programs. Some efforts have been made to push back on this apparent overreach of powers, however to a large extent, the NSA's surveillance capabilities remain intact. On metadata, there is reasonable debate on the extent to which it assists in law enforcement criminal investigations. From a local or state law enforcement perspective, claims that it is not sufficient in solving criminal cases seem quiet plausible, whoever, for the FBI's or NSA's purposes it seems more useful. Nevertheless, it is not possible to encrypt Metadata, and therefore, useful or not, ethical or not, it will always be available to aid law enforcement agencies in their efforts to effectively solve case and appropriately serve justice.

Chapter 3: Alternative Solutions to Required Exceptional Access

Although the landscape seems to be changing in favor of privacy advocates, the government still maintains the ability to use and improve many sophisticated surveillance tools and procedures. Although, these methods alarm privacy advocates, relying on surveillance technology may be one preferable solution to combating going dark that does not weaken existing security infrastructure by

[56] Granick, Jennifer. "NSA's Creative Interpretations Of Law Subvert Congress And The Rule Of Law". *Forbes*. 18 January 2014.
[57] Leahy, Sen. Patrick; Sensenbrenner, Rep. Jim (29 October 2013). "The case for NSA reform". *Politico*. 18 January 2014.

decryption. A recent landmark Harvard study, "Don't Panic", argues that although the use of encryption may present a barrier to surveillance, it may not be impermeable. There are many ways to implement encryption incorrectly. This research claims that Encryption typically does not protect metadata, such as e-mail addresses and mobile device location information that "must remain in plaintext to serve a functional purpose." Moreover, "Data can also be leaked into unencrypted media, through cloud backups and syncing across multiple devices" (Olsen 9). We will see how these weaknesses are, or ought be, exploited and utilized by law enforcement.

On privacy, there have and will always be pockets of communications that are out of reach of surveillance. However, more than ever before areas are becoming increasingly illuminated. Before the digital age, it seems evidence of a crime was just as difficult to come by. Consider the case of assault. If someone murders someone in public, and a third-party witnesses the act from a distance, what information does law enforcement have to convict the criminal, other than a rough physical description? Today, regardless of whether or not metadata provides enough information to convict a suspect, there are surveillance cameras on nearly every block! Even as encryption blocks government access to phone data, we live our lives more on our devices and on the Internet than we have could have before. Even if this information is protected by software, it is nevertheless information that did not exist before the digital age. As technology has progressed, there are those who have and will continue to exploit it to conceal nefarious actions. However, many argue

that claiming we have more privacy than in the past is an inaccurate depiction of the technological landscape.

On this note, the proliferation of surveillance cameras—although tangentially connected to this debate—are peculiarly not openly criticized by many privacy advocates. Perhaps this form of surveillance is being overshadowed by the more surreptitious methods described above. Nevertheless, you don't often hear people making a fuss about the surveillance camera at the traffic light, in the convenience store, or on the city block. Why is that? In all likelihood they will grow coverage and dependability. Perhaps it is because of the distance between the viewer and the suveilled. The surveillance captures you at a distance; it doesn't necessarily track you (yet) or read you messages. But, if well connected, networks of cameras could track your day; from everywhere you go outside of your home. And yet, today they don't seem to have the power to be abused the way metadata, for instance, can be. Surveillance cameras capture robbers, traffic light runners, or traffic collisions. They are only employed after an event has occurred, rather than before or during. Still, the American Civil Liberties Union (ACLU) deplores their proliferation and warns against possible abuses.[58] They argue that studies show the camera don't act as a deterrent to crime (although I believe they are in place to collect evidence than to deter) and that crime rates have not decreased as they have become more prevalent. Nevertheless, video surveillance has proven to be useful in not merely petty theft crimes or traffic accidents, but even in national security threats. Video surveillance

[58] See American Civil Liberties Union, " What's Wrong with Public Video Surveillance", Accessed on February 12, 2017. https://www.aclu.org/other/whats-wrong-public-video-surveillance

spotted the suspects in the Boston Marathon bombings (2013),[59] helped pin down terrorists who carried out the London bombings (2005),[60] and captured the Tucson shooting (2011).[61] When it comes to the normative question "should we allow bulk data collection?" surveillance cameras appear useful, and unlikely to go away anytime soon.

A Deeper Look into Government Mass Surveillance

You may be thinking, "If I am not doing anything illegal, why should I care about the government using mass surveillance?" There are many of those who live straightforward lives who believe there to be no reason the government should or would be targeting them. Because they have nothing to hide, when government agencies such as the NSA secretly gain more powers, it means little to them. They know NSA is just trying to track and catch terrorist plotting against the United States of America. Since the vast majority of American citizens are *not* terrorists, why were the Snowden revelations so disconcerting? In other words, what is problematic for government surveillance agencies gaining more power?

A number of instances in the last century, in which United States government powers were abused, proved to be both unconstitutional and harmful to United States citizens. Significant examples that best demonstrate these trends are

---

[59] See http://www.geekwire.com/2013/security-cameras-helped-catch-boston-marathon-bombers-public-surveillance/

[60] McVeigh, Karen. "How CCTV helped snare failed terrorists", *The Guardian*: July 10, 2007. Accessed on March 5, 2017.

[61] See Ovide Shira."Skype Social media Accounts Hacked by Syrian Electronic Army", *Wall Street Journal*: January 1, 2014. Accessed August 4, 2016. https://blogs.wsj.com/digits/2014/01/01/skype-social-media-accounts-hacked-by-sea/

illustrated by the events that occurred during the Red Scare. The McCarthyism era was dominated by fears and anxieties about Soviet espionage and radical anarchism. Certain prominent cases stand out in history such as *Yates v. United States*[62] and *Watkins v. United States*.[63] In both cases are examples where United States citizens were charged with crimes, later to be overturned by U.S. Supreme Court decision.

It is difficult to find precise number of victims affected by the anti-communist investigations. It is estimated that the number imprisoned is in the hundreds, while ten to twelve thousand lost their jobs. In many cases, simply being subpoenaed by the House Un-American Activities Committee (HUAC) was enough to be fired.

During this period, FBI director J. Edgar Hoover designed President Truman's loyalty-security program, in which FBI agents investigated the backgrounds of countless employees. The scale of such an assignment demanded the expansion of the Bureau to double in size from 1946 to 1952 (Weiner 211). "When the dust cleared, maybe 1 in 10 was found guilty of a deportable offense," says Weiner. "Hoover denied — at the time and until his death — that he had been the intellectual author of the Red Raids"(Weiner 211).

As the anti-communist movement grew it expanded to included homosexuality, and was termed the "Lavender scare". Widely spread FBI surveillance was established intended to identify homosexual government employees.[64] The hunt for homosexuals, who were presumed to be "subversive" by

[62] Yates v. United States, 354 U.S. 298 (1957)
[63] WATKINS v. UNITED STATES, (1957) No. 261 Argued: March 7, 1957
[64] D'Emilio, John and Freedman, Estelle. "Intimate Matters: A History of Sexuality in America", Third Edition. (Chicago: University of Chicago Press, 2012.), p. 316

nature, resulted in thousands being harassed and denied employment.[65] Hoover conflated—and he was not alone—communism with homosexuality. Interestingly, "Both communists and homosexuals had secret coded language that they spoke to each other, and they had clandestine lives, they met in clandestine places, they had secrets."[66] Says Tim Weiner, a Pulitzer Prize winner and New York Times reporter.[67]

The FBI surveillance efforts didn't stop there. Hoover also saw the anti-war protestors and civil rights leaders as "subversives". Tim Weiner explains that these people were enemies of the state (Martin Luther King Jr. in particular. Hoover was determined to surveil King by planting bugs around civil rights leaders (thinking communists had infiltrated the civil rights movement). "Hoover had his intelligence chief bugged King's bedroom, and then sent the civil rights leader a copy of the sex recordings his intelligence chief… and sent [the tapes] to colleges to keep him off campus" Weiner says.[68] He continues to explain how, "[Edgar] decided up to a point ... where the boundaries of the law [were] when it came to black bag jobs, break-ins, bugging, surveillance, the constitutionality of gathering secret intelligence on America's enemies — both real and imagined."

Moreover, there have been numerous abuses of power in the past decade. Along with the exploitations of the Patriot Act discussed previously, the No-Fly List (a list to track people the government prohibits form traveling because they have

---

[65] Ibid. p. 316

[66] See Weiner, Tim. "The History of the FBI's Secret 'Enemies' List" NRP: heard on Fresh Air. February 14, 2012. Accessed on March 13, 2017.

[67] Interestingly, many historians argue and speculate that J. Edgar Hoover was, in fact, a homosexual: Terry, Jennifer. "An American Obsession: Science, Medicine, and Homosexuality in Modern Society". University of Chicago Press. (1999) p. 350

[68] Weiner, Tim.

been labeled as security risks) is of growing controversy. There are more than 47,000 names as of 2013.[69] The American Civil Liberties Union (ACLU) has long criticized the No Fly List and similar lists on the asserting that the government has not provided a constitutionally adequate means of allowing individuals to challenge their inclusion on the list. The ACLU states that "constitutional rights are at stake when the government stigmatizes Americans as suspected terrorists and bans them from international travel.[70] The list is known for making errors, most notably with Senator Ted Kennedy, who was flagged trying to fly from Boston to Washington.[71]

Although much has changed in the past century, private citizens and government officials alike are facing new fears today in regards to extreme Islamic terrorism and immigration. In a panel discussion here at the University of Texas, Christopher Soghoian argues that the government's problem with widespread encryption for private use is really about *new* people having access to communications security (where as FBI, presidents, and law enforcement agencies have been using encrypted phones for decades).[72] He views the issue not only as a problem for privacy advocates (like himself) but also has a problem of equality and racial justice. He says, "I view [going dark] as a hand ringing of those in power, who have long had encryption, who are upset that those without power are about to get encryption… I think we should have an honest conversation and say this is not new people having access to communications security because the FBI directors' had an

[69] See http://www.foxnews.com/travel/2015/09/09/8-ways-can-end-up-on-no-fly-list.html
[70] Seehttps://www.aclu.org/issues/national-security/privacy-and-surveillance/watchlists
[71] See http://www.factcheck.org/2015/12/ted-kennedy-and-the-no-fly-list-myth/
[72] Soghoian, Christopher. *Session 1: The "Going Dark" Encryption Debate*. Robert Strauss Center. Feb 12, 2016 <https://www.youtube.com/watch?v=B_7CWSgr1Vg>

encrypted phone for decades, the presidents' had encrypted phone for decades, and law enforcement over the last ten years have been increasingly moving from open air radio communications to encrypted radios. I view this as a problem of equality and racial justice, which isn't apart of the current debate." Soghoian is a strong privacy advocate and definitely on the far side of that of the spectrum. At moments he may seem overzealous about the importance of strong encryption, but I think he raises a very interesting point here about the purpose of surveillance in law enforcement. He claims that African Americans and Muslims, in particular, are the most surveilled groups of people in the United States, and raises questions regarding the true extent to the government's fears of going dark. It is worth keeping in mind as we are dealing with issuing of border control, refugees, and immigration today (which are becoming more and more, I believe, evocative of the Hoover era.

Many experts argue the metaphor "going dark" is misleading and does not accurately depict the world we are living in. They claim, in actually, the digital landscape is "going bright" because we are—as privacy law professor Peter Swire terms— in "the golden age of surveillance."[73] Not only have we seen United States government agencies create and expand their surveillance programs in the last decade, but like all technology, surveillance technology has before cheaper and more readily available. One great example of this is the IMSI-catcher, also known as a StingRay, which tracks and intercepts telecommunications. You might recognize it from that police scene in any movie, ever. As Christopher Soghoian elucidates, "Your

[73] Peter Swire and Kenesa Ahmad, "'Going Dark' Versus a Golden Age of Surveillance," Center for Democracy & Technology, November 28, 2011.

cell phone is not secure. If you make a telephone call today, someone standing outside your house with about $500 worth of hardware can listen to your calls."[74] This could be a police department, a stalker, a criminal, a foreign government, or a competitor of yours seeking to get information. He continues to explain this has how it has been for more that 20 years, and the government was initially the only party capable of this type of "wiretapping". However, today—as costs of technologies drop— "we have truly democratized surveillance capabilities where anyone can either go onto Alibaba (a Chinese equivalent of EBay) and by a StingRay for $2000 off the shelf, or build one themselves".[75] In this chapter we will continue our discussion of government surveillance in regards to solutions that do not require any decryption or weakening of current security systems.

The Internet of Things

> Everyday objects are increasingly becoming embedded with technology that connects it to networked servers (the Internet) in what is becoming known as the Internet of Things (IoT). According to expert observers "the Internet of Things has the potential to fundamentally shift the way we interact with our surrounding" (Olsen 13). This would include at home, at work, in our cars, in shopping centers, and on public streets. Moreover, the "IoT market is forecast to grow into a multitrillion dollar industry within the next ten years" (Olsen 13). This will significantly change how members of society interact

[74] See https://www.youtube.com/watch?v=B_7CWSgr1Vg 19:45
[75] Ibid.

> with each other and the objects and devices around them. To paint a picture, IoT appliances and products can be "televisions and toasters to bed sheets, light bulbs, cameras, toothbrushes, door locks, cars, watches, and other wearables." All of these objects can and will be packed with wireless technology that will connect to the Internet (Olsen 13). This emerging market of objects will not only revolutionize the computing industry, but will also create prime mechanisms for surveillance—" alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark – so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become" (Olsen 12).

A number of companies are developing business strategies and products. Phillips, GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all working on products embedded with IoT technology. These devices include microphones, speakers, accelerometers, magnetometers, proximity sensors, barometers, infrared sensors, and fingerprint readers to name a few. A familiar example of an IoT that has existed for decades is OnStar: a subsidiary of General Motors that provides communications, navigation, and remote diagnostics systems. These devices will all be connect and communicate with each other, and with their respective retailer cloud servers.[76] These new technologies will provide law

[76] See David Linthicum, "Thank the cloud for making big data and IoT possible," InfoWorld, January 16, 2015, http://www.infoworld.com/article/2867978/cloud-computing/thank-the-cloud-for-making-big-data-and-internetof-things-possible.html.

enforcement with additional information and evidence as they become more and more unavoidable.

For example, Samsung has developed smart TVs built with voice command capabilities since 2015. Samsung's privacy policy instructs users to "be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through you use of the Voice Recognition."[77] Because voice recognition is a "computationally intensive task", the processing power demanded for this task is too great for modern television technology, so these companies utilize cloud infrastructure through a network connection to send the voice data to a remote serve to process, interpret, and relay data back to the television (Olsen 14). Simple voice commands such as, "go to channel 52" can be computed by the television. However, more complex voice commands are required to be sent to Samsung's servers.

As a result, law enforcement or intelligence agencies could start to request Samsung, and similar companies of networked devices, to hand over data with legally obtained warrants, or even "push an update or flip a digital switch to intercept the ambient communications of a target" (Olsen 14). If these predictions are as accurate as they appear, the Internet of Things will continue to create a world of information law enforcement can use. This example isn't necessarily the answer to the going dark problem. It is meant to provide a viable alternative path for law

[77] See Samsung, "Samsung Privacy Policy – SmartTV Supplement," http://www.samsung.com/sg/info/privacy/smarttv.html (accessed October 26, 2015).

enforcement to pursue, which isn't mandating access to telecommunication companies.

Lawful Hacking Solution as an Alternative Solution

As we have seen over the past decade, the FBI is not only interested in accessing communication devices, they are also concerned with accessing communication networks. Valerie Caproni, General Counsel of the FBI, said in a Congressional testimony:

> Methods of accessing communications networks have similarly grown in variety and complexity. Recent innovations in hand-held devices have changed the ways in which consumers access networks and network-based services. One result of this change is a transformation of communications services from a straightforward relationship between a customer and a single CALEA-covered provider (e.g. customer to telephone company) to a complex environment in which a customer may use several access methods to maintain simultaneous interactions with multiple providers, some of whom may be based overseas or are otherwise outside the scope of CALEA.
>
> As a result, although the government may obtain a court order authorizing the collection of certain communications, it often serves that order on a provider who does not have an obligation under CALEA to be prepared to execute it.

Similar to the evolution of the telecommunication industry, technology has had a similar effect on the relationship between the government and Internet provides. Steven M. Bellovin explains in "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet", that over the last three decades, "we have moved from a circuit-switched centralized communications network…run by a monopoly provider, to an Internet Protocol (IP) base decentralized network run by thousands of providers" (Bellovin 5). This change gave rise to the need for the Communications Assistance for Law Enforcement Act (CALEA). This Act, passed in 1994, was designed to enhance the ability of law enforcement agencies to conduct lawful interception of communication by required that telecommunications carriers and manufactures of telecommunications design their systems with built-in vulnerabilities fro targeted surveillance. It has since been extended to cover broadband Internet and VoIP.[78] As the providers multiplied, and communications become encrypted end-to-end, Bellovin explains, the CALEA's ability to legally authorize wiretaps may be impeded. Similar to requiring access to telecommunication devices, the FBI's preferred solution is "requiring that social-networking Web sites and providers of VoIP, instant messaging, and Web e-mail alter their code to ensure their products are wiretap-friendly".[79] According to Steve

[78] VoIP (or Voice over Internet Protocol) is a technological method of delivering voice communications and multimedia over the Internet (IP) networks. A prevalent example of this technology is SKYPE.

[79] See Declan McCullagh, FBI: We Need Wiretap-Ready Web Sites—Now, CNET (May 4, 2012), http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/

M Bellovin, vulnerability is "a weakness in a system that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system" (23). Vulnerabilities can be bugs, or defects, in the code, or misconfigurations, such as not changing a default password or running open, unused services. In addition he explains that "another common type of vulnerability results from not correctly limiting input text (this is also known as not sanitizing input) (23).

We know that our communications systems today are under attack and require security systems to ensure the protection of sensitive information, whether it is government, corporate, or personal. Thus, mandating access points (also called wiretaps) on communications tools is ostensibly an opportunity for increased exploitation by the enemy. Furthermore, the general clandestine nature of CALEA mandates increase security risks. As Ben Adida explains in "CALEA II: Risks of Wiretap Modifications to Endpoints", the most dangerous cyber-attacks are those "which not only compromise a system but also evade detection. This is precisely the objective of a government surveillance solution"(Adida 5). Thus, adding wiretap capabilities to Internet based networks can be uniquely dangerous precisely because they are designed to be unknown in application. Adida further explains that "wiretaps are designed to be kept secret from both the parties involved in the communication and also from anyone else that does not have a 'need to know' in order to execute the tap" (Adida 5). Mandating wiretapping capabilities is a dangerous solution because it increases the possibility that a malicious hacker could

intercept communications with lower risk of discovery. In other words, it would the FBI would be opening doors for both themselves and the enemy.

There are, after all, other ways of ways of going after communications content than providing law enforcement with mandated access to encrypted communications. Although the majority of technology experts warn against created any new wiretapping capabilities, there are some who suggest exploiting those that already exist is viable solution. It sounds somewhat dubious, in essence, as it requires law enforcement agencies to commit the same actions as malicious hackers. Nevertheless, no one complained when the FBI broke into Syed Farook's (San Bernardino terrorist) phone with the help of a third party, as this is essentially the same solution in a different context. Furthermore, it is important to keep in mind that in doing, this strategy would be more expensive and require more and more time and resources into conducting targeting seizure of evidence. In addition, local and state law enforcement agencies tend to have fewer resources and are technologically less advanced than federal agencies, and would therefore rely more and more on their assistance into criminal investigations. Nevertheless, this approach is a tradeoff enabling the vast majority of communications to remain and continue to be secure.

Another simple way for law enforcement to gain access to network vulnerabilities is to buy them. Software companies and developers are constantly trying to minimize vulnerabilities in their systems, and as such, there has become a market for finding those vulnerabilities. Companies rely on other software engineers to find these exploits in order to patch them as quickly as possibly

(Bellovin 41). The overt vulnerabilities marketplace started in 2004 when Mozilla launched the fist bug-bounty program.[80] The program pays security researchers for vulnerabilities they discover. Many other companies have sprung with similar bug-bounty programs. Bellovin reveals that "Many legitimate security research firms have made finding vulnerabilities and developing exploits for sale part of their business model" and that "prices range from $20 to $250,000 with exclusive access to a critical zero-day generally the most expensive"(42). A zero-day is a vulnerability discovered and exploited prior to public awareness or disclosure to the vendor. Furthermore reports suggest that national government intelligences agencies have become major buyers.[81] These companies include: Vupen, Revuln, and Vulnerabilities-Lab and offer not only working exploits and vulnerabilities, but also offer special targeted exploits developed for additional fees (Bellovin 43).

Lastly, vulnerabilities will always exist. This is do to the fact that security codes are write by human beings, and as such are prone to mistakes. Bellovin notes that "if it has not been programmed that way—if there is virtually any imperfection in code—a bug will result" (27). Further more A National Research Council study described the situation this way:

> [An] overwhelming majority of security vulnerabilities are caused by "buggy" code. At least a third of the Computer Emergency Response Team (CERT)

---

[80] See Press Release, Mozilla Foundation Announces Security Bug Bounty Program (Aug. 2, 2004), available at https://www.mozilla.org/en-US/press/mozilla-2004-08-02.html.

[81] Nicole Perlroth & David E. Sanger, Nations Buying as Hackers Sell Flaws in Computer Code, N.Y. TIMES, July 13, 2013, https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackerssell-computer-flaws.html.

> advisories since 1997, for example, concern inadequately checked input leading to character string overflows (a problem peculiar to C programming language handling of character strings). Moreover, less than 15 percent of all CERT advisories described problems that could have been fixed or avoided by proper use of cryptography. [82]

As software program become more and more complex the possibilities of testing and finding bugs decreases. The ability to produce an error-free code is "the Holy Grail of systems development: heavily desired but unattainable. Although, vulnerabilities are limited, and not exactly cost effective, they appear to be the only practical solution that doesn't pose a direct threat to national security. There are a number of question that arise, however, using this strategy of combatting going dark both regulatory and ethically such as: Does local and even state law enforcement agencies have the technical sophistication to develop and use exploits? If not, how should this be handled? And should the FBI take larger role? Moreover, Should law enforcement even be participating in a market where many of the sellers and other buyers are themselves criminals? Does the FBI have an ethical obligation to share knowledge of vulnerabilities? In the free market it is common practice to expose any known vulnerabilities (at least for a price), but in the governments best interest, they would want these vulnerabilities to remain exploitable for as long as possible. In doing so, would be acting unethically by keeping vulnerabilities disclosed, and would this not only increase risk, but also hinder innovation? These questions are,

[82] TRUST IN CYBERSPACE 110 (Fred B. Schneider ed., 1999).

although beyond the scope of this paper, difficult to answer. It seems that any solution to going dark will not only be complex and multifaceted, but also not without some costs.

Conclusion

The debate over privacy and security, in actuality, is a tradeoff between more security and less security. From a policy perspective, this debate raise difficult questions regarding data privacy, national security, economics, technology, ethics, and mass surveillance. We are forced to consider whether providing access to encrypted communications to help prevent terrorism and aid in criminal investigation is worth increasing our vulnerability to cyber threats. The findings of this paper demonstrate the inherent dangers involved in weakening encryption, on any level, and the practical consequences of doing so. Based on the findings of leading security technologists, I conclude that any decryption should not be considered as a practical solution from both technological or policy perspective, as it would position everyone at risk of cyber threats, while those who wish to hide, will always have other means of doing so technologically speaking.

At the same time, from a civil liberties perspective, we must consider whether preventing the government from gaining access to communications under circumstances strike the right balance between privacy and security, particularly when terrorists and criminals seek to use encryption to evade government surveillance. Ultimately, mandating access to data and communications is a simple

solution for a simple problem, however going dark is very complex, and requires a multifaceted and refined solutions. Widespread encryption forces those listening—whether it is the NSA, FBI, foreign governments, criminals or terrorist—to be much more deliberate. As for the going dark metaphor, it seems as through we are not entirely "going dark", and yet we are not completely bright either. Both the "going dark" metaphor of FBI Director James Comey, and the contrasting "golden age of surveillance" metaphor of privacy law professor Peter Swire focus on the value of data to law enforcement, which this paper did not determine to be understated. The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense, the government is losing some surveillance opportunities. However, our stance is that there just because there are those who use encryption in nefarious ways, doesn't mean we should allow policy to put us all at risk. Although it comes at a cost, the most constructive strategy moving forward, we conclude, involves the combination of technological developments and lawful hacking methods that are likely to continue to fill the gaps of going dark and ensure that the government will gain new opportunities to gather critical information.

Works Cited

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Glimore, Mathew Green, Susan Landau, Peter G. Neumann, Ronald Rivest, Jeffrey Schiller, Bruce Schneier, Michael Specter, and Daniel Weitzner. "Keys Under Doormats: Mandating insecurity by requiring government access to all Data Communications" Massachusetts Institute of Technology, Cambridge. July 6, 2015.

Adida, Ben, Collin Anderson, Annie Anton, et al., "CALEA II: Risks of Wiretap Modifications to Endpoints," May 17, 2013.

American Civil Liberties Union, " What's Wrong with Public Video Surveillance", Accessed on February 12, 2017. https://www.aclu.org/other/whats-wrong-public-video-surveillance

American Library Association, "USA PATRIOT Act and Libraries, enacted June 29, 2005", American Library Association: Chicago, 2017.

Andy Greenberg, "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," WIRED, November 18, 2014. http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

Apple, Inc., "iOS Security Guide: iOS 8.1 or later,"Apple.com/Security: October 2014

Apple, Inc., "IOS Security": May 2016. Apple.com/Security: Accessed on November 11, 2016 https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Ball, James. "NSA collects millions of text messages daily in 'untargeted global sweep" The Guardian: January 16, 2014. Accessed on November 23, 2016.

https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

Bankston, Kevin, Amy Hess, Daniel Conley, Jon Potter, Matthew Blaze, "Encryption Technology & Potential U.S. Policy", Congressional Hearing: April 29, 2015. https://www.youtube.comwatch?v=zk78_zmH4QI

Bankston, Kevin. "Encryption Technology and Possible U.S. Policy Responses", (Before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform). April 29, 2015.

Barret, Devlin, Evan Perez. "Shooting Captured on Surveillance Video*", The Wall Street Journal*: Dow Jones, Inc. January 9, 2011. Accessed on March 5, 2017. https://www.wsj.com/articles/SB10001424052748704482704576072020422761968

Blaze, Matt. "Encryption Technology and Possible U.S. Policy Responses" (Before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform). April 29, 2015.

Blaze, Matt. "Protocol Failure in the Escrowed Encryption Standard", AT&T Bell Laboratories, August 20, 1994.

Blaze, Matt. "Protocol Failure in the Escrowed Encryption Standard", Proceedings of the 2nd ACM Conference on Computer and Communications Security: August 20, 1994.

Blaze, Matt. "U.S. House of Representatives Committee on Government Oversight and Reform Information Technology Subcommittee Encryption Technology and Possible U.S. Policy Responses," Washington D.C. April 29, 2015.

Chris Wysopal, Chris Eng. "Static Detection of Application Backdoors", Veracode, Inc: Burlington, MA. 2007.

Comey, James "Directory Comey Discusses Investigative Challenges in Light of New Methods of Electronic Communications" Fbi.org. March 1, 2016. Accessed August 23, 2016. https://www.fbi.gov/news/stories/director-comey-discusses-investigative-challenges-in-light-of-new-methods-of-electronic-communication

Comey, James. "Expectations of Privacy: Balancing Liberty and Security and Public Safety Center", Study of American Democracy Biennial Conference, Kenyon College: Gambier, Ohio *April 6, 2016.*

Comey, James. "FBI Director Comments on San Bernardino Matter", LawFare Blog: FBI National Press Office, February 21, 2016.

Comey, James. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" The Brookings Institution: Washington, D.C. October 16, 2014.

Comey, James. "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption," Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, July 8, 2015.

Comey, James. "The FBI's Approach to the Cyber Threat", Symantec Government Symposium: Washington, D.C. August 30, 2016. Accessed January 13, 2017 https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat

Conley, Daniel. "Encryption Technology and Possible U.S. Policy Responses" (Before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform). April 29, 2015.

Cook, Tim. "Message to Our Customers", Apple.com: Accessed December 2, 2016. http://www.apple.com/customer-letter/

Cook, Tim. “We Believe Security Shouldn’t Come at the Expense of Individual Privacy” Apple.com/Privacy. Accessed on October 23, 2016. https://www.apple.com/privacy/government-information-requests/

David Linthicum, “Thank the cloud for making big data and IoT possible,” InfoWorld, January 16, 2015, Accessed on March 20, 2017. http://www.infoworld.com/article/2867978/cloud-computing/thank-the-cloud-for-making-big-data-and-internetof-things-possible.html.

Decker, Eileen, Patricia Donahue, Tracy Wilkison. “Government’s Reply In Support of Motion to Compel And Opposition to Apple Inc.’s Motion To Vacate Order”, United States District Court For the Central District of California, March 22, 2016.

Demopoulos, Ted. “Symmetric Key in Use”, 2008. Accessed March 14, 2017. http://securitycerts.org/review/symmetric-key-in-use.htm

Derix, Steven. “NSA Infected 50,000 Computer Networks with Malicious Software”, nrc.nl: November 2013. Accessed January 14, 2017.

Diffie, Whitfield, Hellman, Martin E. “Exhaustive Cryptanalysis of the NBS Data Encryption Standard”, The Institute of Electrical and Electronics Engineers, Inc. California: June 1977.

Editorial Staff, “How to Find a Backdoor in a Hacked WordPress Site and Fix It”, *Wpbeginner Blo*g: November 28, 2012. http://www.wpbeginner.com/wp-tutorials/how-to-find-a-backdoor-in-a-hacked-wordpress-site-and-fix-it/

FindLaw, *John Watkins v. United States* 354 U.S. 178 (1957).

Gellman, Barton, Ashkan Soltani. “NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say”. *The Washington Post*: October 31, 2013. Accessed September 23, 2016.

Gellman, Barton, Ashkan Soltani. “NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say”, The Washington Post: October 30, 2013. Accessed on November 23, 2016.

Gorman, Siobhan, Jennifer Valentiono-Devries. "New Details Show Broader NSA Surveillance Reach - Programs Cover 75% of Nation's Traffic, Can Snare Emails". The Wall Street Journal: August 21, 2013.

Granick, Jennifer. “NSA's Creative Interpretations Of Law Subvert Congress And The Rule Of Law”, *Forbes*: 18 January 2014.

Greenberg, Andy “WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users,” WIRED, November 18, 2014.

Grossman, Lev. “Inside Apple CEO Tim Cook’s Fight with the FBI”, TIME*:* California*,* March 17, 2016. Accessed October 18, 2016.

Hess, Amy. “Statement Concerning Encryption and Cybersecurity For Mobile Electronic Communication Devices”, Before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform, April 29, 2015.

Johnson, Jeh Charles. “Budget-in-Brief Fiscal Year 2016” U.S. Department of Homeland Security: 2016.

Kiely, Eugene. “Ted Kennedy and the No-Fly List Myth”, *FactCheck.Org,* December 8, 2015. Accessed on March 21, 2017. http://www.factcheck.org/2015/12/ted-kennedy-and-the-no-fly-list-myth/

Leahy, Sen. Patrick, Sensenbrenner, Rep. Jim. "The case for NSA reform", *Politico*: 18 January 2014.

Levy, Steve. “How the Code Rebels Beat the Government Saving Privacy in the Digital Age”, Penguin Group: New York, 2001.

MacAskill, Ewen“GCHQ taps fibre-optic cables for secret access to world's communications” *The Guardian*: June 21, 2013. Accessed November 8, 2016.

McVeigh, Karen. “How CCTV helped snare failed terrorists”, *The Guardian*: July 10, 2007. Accessed on March 5, 2017. https://www.theguardian.com/uk/2007/jul/10/terrorism.world2

Nakashima, Ellen. “Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say” The Washington Post: May 20, 2013. Accessed February 22, 2017.

Olsen, Matt, Bruce Schneier, and Jonathan Zittrain. “Don’t Panic. Making Progress on “Going Dark Debate”. Berkman Center Harvard University: 2016.

Ovide Shira.”Skype Social media Accounts Hacked by Syrian Electronic Army”, *Wall Street Journal*: January 1, 2014. Accessed August 4, 2016. https://blogs.wsj.com/digits/2014/01/01/skype-social-media-accounts-hacked-by-sea/

Potter, Jon. “Data Protection, Law Enforcement and the Global Digital Economy”, Encryption Technology and Possible U.S. Policy Responses Before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform: April 29, 2015.

Prevelakis, Vassilis, Diomidis Spinellis, "The Athens Affair," IEEE Spectrum, June 27, 2007.

Richtel, Matt. "Hacker Group Says Program Can Exploit Microsoft Security Holes" *New York Times* August 4, 1998. Retrieved April 24, 2007.

Sanger, David. "Signaling Post-Snowden Era, New iPhone Locks Out NSA", *The New York Time*s, September 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the- nsa-signaling-a-post-snowden-era- .html.

Scahill, Jeremy, Begley, Josh. "The Great Sim Heist: How Spies Stole The Keys to the Encryption Castle" The Intercept Blog: February 19, 2015. Accessed December 2, 2016. https://theintercept.com/2015/02/19/great-sim-heist/

Schneier, Bruce. "Security or Surveillance?" Lawfare Blog, February 1, 2016. Accessed on September 12, 2016. https://lawfareblog.com/security-or-surveillance

Sineubko, Denis. "Unmasking "Free" Premium WordPress Plugins. *Sucuri Blog*. March 26, 2014. Accessed October 17, 2016. https://blog.sucuri.net/2014/03/unmasking-free-premium-wordpress-plugins.html

Snowden, Edward, "XKeyscore", xkeyscore@nsa, February 25, 2008. Accessed on November 8, 2016. https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf

Soghoian, Christopher. "FIC 2016- Keynote Christopher Soghoian", International forum of Cybersecurity: Feb 10, 2016. Accessed on January 21, 2017. <https://www.youtube.com/watch?v=kqWn-DF-ln8>

Soghoian, Christopher. “FIC 2016-Keynote Christopher Soghoian”, International Forum on Cybersecurity: February 10, 2016. Accessed September 23, 2016. https://www.youtube.com/watch?v=kqWn-DF-ln8

Soghoian, Christopher. Session 1: The "Going Dark" Encryption Debate – Robert Strauss Center. Accessed on March 12, 2017. Accessed on November 12, 2016. <https://www.youtube.com/watch?v=B_7CWSgr1Vg>.

Soghoian, Christopher. *Session 1: The "Going Dark" Encryption Debate*. Robert Strauss Center. Feb 12, 2016 <https://www.youtube.com/watch?v=B_7CWSgr1Vg>

Soper, Taylor. “Security cameras help catch Boston Marathod Bombers; what’s your take on public surveillance?” *Geekwire*: April 20, 2013. Accessed on March 5, 2017.

Staff. "NSA Slides Explain the PRISM Data-Collection Program". *The Washington Post*: June 6, 2013.

Stamos, Alex. “User-Focused Security: End-to-End Encryption Extension for Yahoo Mail,” Yahoo Blog, March 15, 2015.http://yahoo.tumblr.com/post/113708033335/user-focused-security-end- to-end-encryption.

Swire, Peter, Kenesa Ahmad, “‘Going Dark’ Versus a Golden Age of Surveillance,” *Center for Democracy & Technology*, November 28, 2011.

Timberg, Craig. “Newest Androids will join iPhones in offering default encryption, blocking police,” The Washington Post, September 18, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newestandroids-will-join-iphones-in-offering-default-encryption-blocking-police/.

Tuchman, Walker. “A brief history of the data encryption standard", Internet besieged: countering cyberspace scofflaws. ACM Press/Addison-Wesley Publishing Co. New York. 1997.

USA Patriot Act, “H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001” *House - Judiciary; Intelligence (Permanent); Financial Services; International Relations; Energy and Commerce; Education and the Workforce; Transportation and Infrastructure; Armed Services*. 2001.

Vance, Cyrus. “Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy”, (Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on the Judiciary), Washington D.C. July 8, 2015.

Vinson, Roger. “In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Business Network Services, Inc. On Behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services” United States Foreign Intelligence Surveillance Court: Washington, D.C. 2013.

Ware, Willis H. “Security Controls For Computer Systems: Report of Defense Science Board Task Force on Computer Secuirty – RAND Report R-609-1” Rand: Santa Monica, CA, October 10, 1979.

Weiner, Tim. “The History of the FBI’s Secret ‘Enemies’ List” NRP: heard on Fresh Air. February 14, 2012. Accessed on March 13, 2017.

Yates v. United States 354 U.S. 298 (1957).

Biography

Jackson Stein was born in Dallas, TX on March 27, 1995 and graduated from Hillcrest High School in 2012. He took a gap year living in Israel for 9 months studying Middle Eastern conflict and volunteering teaching English in underdeveloped elementary schools. He enrolled in the Plan II Honors program at the University of Texas at Austin in 2013 and joined the ZBT Lambda Fraternity. He graduated in 2017 and plans to begin a career in wealth management in Austin, TX.